

BEST AVAILABLE COPY

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平11-196081

(43)公開日 平成11年(1999)7月21日

(51) Int.Cl.⁶
 H 04 L 9/08
 G 09 C 1/00
 H 04 L 9/14

識別記号
 6 3 0

F I
 H 04 L 9/00
 G 09 C 1/00
 H 04 L 9/00
 6 0 1 A
 6 3 0 E
 6 0 1 E
 6 4 1

審査請求 有 請求項の数4 FD (全16頁)

(21)出願番号 特願平9-368942

(22)出願日 平成9年(1997)12月26日

(71)出願人 597174182
 株式会社高度移動通信セキュリティ技術研究所
 神奈川県横浜市港北区新横浜三丁目20番地
 8

(72)発明者 安賀 潤
 神奈川県横浜市港北区新横浜三丁目20番地
 8 株式会社高度移動通信セキュリティ技術研究所内

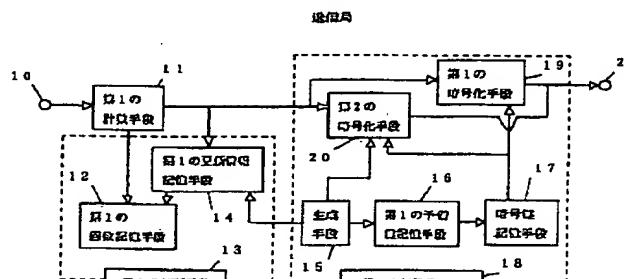
(74)代理人 弁理士 役 昌明 (外1名)

(54)【発明の名称】 暗号通信装置

(57)【要約】

【課題】 共通(秘密)鍵ブロック暗号を暗号通信と暗号鍵配達に用いる暗号通信装置において、安全かつ簡単に更新鍵を配達する。

【解決手段】 鍵更新の際、送信局において、予備鍵を新規暗号鍵とし、生成手段15で生成した予備鍵を新規予備鍵とし、予備鍵を暗号鍵で暗号化して送信し、その後、送信データを暗号鍵で暗号化して送信する。受信局においては、予備鍵を新規復号鍵とし、受信暗号化鍵を復号化して新規予備鍵とし、その後、受信暗号化データを復号化する。定期的に更新される予備の鍵を常に用意することにより、同じ鍵を暗号通信と鍵配達に一定の安全性で使用できる。鍵配達に使用する鍵は常に未使用なので安全性が高く、かつ配達用の鍵を管理(生成・更新)する手間を省くことができる。また、予備鍵や平文に応じて鍵更新のタイミングを決定することにより、予め送信局と受信局の間で鍵更新のタイミングを決定する必要が無く、かつ鍵更新のタイミングがランダムになるので、解読を容易にする情報が盗聴者に特定し難くなる。



【特許請求の範囲】

【請求項1】 送信局と受信局からなる暗号通信装置であって、前記送信局は、暗号鍵を記憶する暗号鍵記憶手段と、第1の予備鍵を記憶する第1の予備鍵記憶手段と、データを前記暗号鍵を用いて暗号化する第1の暗号化手段と、前記第1の予備鍵を前記暗号鍵を用いて暗号化する第2の暗号化手段と、前記第1の予備鍵を生成する生成手段と、前記第1の予備鍵を新規暗号鍵として前記暗号鍵記憶手段に転送し、前記生成手段により生成された予備鍵を新規第1の予備鍵として前記第1の予備鍵記憶手段に転送し、前記第2の暗号化手段の結果を出力し、その後前記第1の暗号化手段の結果を出力することを制御する第1の制御手段とを備え、前記受信局は、復号鍵を記憶する復号鍵記憶手段と、第2の予備鍵を記憶する第2の予備鍵記憶手段と、暗号化データを前記復号鍵を用いて復号化する第1の復号化手段と、前記第2の暗号化手段の結果を前記復号鍵を用いて復号化する第2の復号化手段と、前記第2の予備鍵を新規復号鍵として前記復号鍵記憶手段に転送し、前記第2の復号化手段の結果を新規第2の予備鍵として第2の予備鍵記憶手段に転送し、その後前記第1の復号化手段の結果を出力することを制御する第2の制御手段とを備えることを特徴とする暗号通信装置。

【請求項2】 送信局における前記第1の暗号化手段が、前記暗号鍵を用いて暗号化データを復号化し、受信局における前記第1の復号化手段が、前記復号鍵を用いてデータを暗号化することを特徴とする請求項1記載の暗号通信装置。

【請求項3】 前記受信局が、前記第2の暗号化手段の結果を記憶する暗号化予備鍵記憶手段と、前記第2の暗号化手段の結果を暗号化予備鍵記憶手段に転送し、前記第2の復号化手段の結果を新規復号鍵として前記復号鍵記憶手段に転送することを制御する第2の制御手段とを備えることを特徴とする請求項1記載の暗号通信装置。

【請求項4】 前記送信局は、送信回数を計数する第1の計数手段と、前記送信回数と前記送信回数上限値を記憶する第1の回数記憶手段と、更新情報を記憶する第1の更新情報記憶手段と、前記送信回数と前記送信回数上限値を調べ、前記送信回数上限値が一定値以下ならば前記送信回数上限値に一定値の加算を行ない、前記送信回数と前記送信回数上限値が等しいならば前記更新情報を前記送信回数上限値へ書き込み、更新開始の通知を行ない、その後新規更新情報の前記更新情報記憶手段への転送を行なう第1の判断手段とを備え、前記受信局は、受信回数を計数する第2の計数手段と、前記受信回数と前記受信回数上限値を記憶する第2の回数記憶手段と、前記受信回数と前記受信回数上限値を調べ、前記受信回数上限値が一定値以下ならば前記受信回数上限値に一定値の加算を行ない、前記受信回数と前記受信回数上限値が等しいならば前記更新情報を前記受信回数上限値へ書き

込み、更新開始の通知を行ない、その後新規更新情報の前記更新情報記憶手段への転送を行なう第2の判断手段とを備えることを特徴とする請求項1記載の暗号通信装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、送信局と受信局からなる暗号通信装置に関し、特に、共通（秘密）鍵ブロック暗号を暗号通信と暗号鍵配送に用いた暗号通信装置における鍵更新装置に関する。

【0002】

【従来の技術】 従来の共通（秘密）鍵ブロック暗号を、暗号通信と暗号鍵配送に用いた暗号通信装置は、鍵更新のための鍵配送方式として、更新用の新しい鍵を、鍵更新前まで使用していた鍵で暗号化して配送する（例えば、特開昭60-10834号公報）か、別に用意した配送用の鍵で暗号化して配送する（例えば、特開昭62-104238号公報）か、過去に使用された鍵で暗号化して配送する（例えば、特開平1-225251号公報）という手段を用いていた。

【0003】 また、鍵更新を行なうタイミングとして、暗号通信のたびや送信局か受信局から更新要求があったとき、または鍵の使用が一定時間に達したとき（例えば、特開昭62-181643号公報）等に鍵更新を行なっていた。

【0004】 図11と図12は、従来の暗号通信装置として、前記先行技術をいくつか組み合わせた例を示し、図11は送信局の例、図12は受信局の例を示す。点線で括られた範囲の各手段は判断手段または制御手段により制御される。

【0005】 従来の暗号通信装置では、鍵更新を行なうタイミングとして、（A）暗号通信のたびに鍵更新を行なう方式や、（B）送信局か受信局から更新要求があったときに鍵更新を行なう方式や、（C）鍵の使用が一定時間に達したとき等に鍵更新を行なう方式があった。

（A）と（B）の2方式が、図11と図12において、51、52、53、71、72、73が存在しない場合に対応し、（C）の方式が、図11と図12において、51、52、53、71、72、73が存在する場合に対応する。

【0006】 従来の（A）方式暗号装置の場合、鍵の更新のタイミングを決定する手段は必要でない。

【0007】 （B）方式暗号装置の場合、鍵の更新のタイミングを決定する手段が存在しないので、送信局または受信局のユーザーは任意の手段を用いてタイミングを決定する必要がある。任意の手段としては、通信時間で更新するならばタイマー、送受信回数で更新するならばカウンター等が考えられる。

【0008】 （C）方式暗号装置の場合、従来の送信局では、第1の計数手段51で計数された送信回数が、第1の回数記憶手段52に記憶され、第1の判断手段53が前記

送信回数と第1の回数記憶手段52に記憶された送信回数上限値を比較して等しければ第1の制御手段60に更新開始を通知する。また、従来の受信局では、第2の計数手段71で計数された受信回数が、第2の回数記憶手段72に記憶され、第2の判断手段73が前記受信回数と第2の回数記憶手段72に記憶された受信回数上限値を比較して等しければ第2の制御手段77に更新開始を通知する。

【0009】従来の暗号通信装置では、鍵更新のための鍵配達方式として、更新用の新しい鍵を、(D) 鍵更新前まで使用していた鍵で暗号化して配達するか、(E) 別に用意した配達用の鍵で暗号化して配達するか、過去に使用された鍵で暗号化して配達するという手段を用いていた。(D) が、図11と図12において、58、76の各手段が存在しない場合に対応し、(E) 方式が、図11と図12において、58、76の各手段が存在する場合に対応する。

【0010】(D) 方式の場合、従来の送信局では、更新開始の通知を受けた第1の制御手段が以下の制御を行なう。第2の生成手段57で生成された新しい鍵を暗号鍵記憶手段55に記憶された既に暗号通信に使用してきた暗号鍵を用いて第2の暗号化手段59で暗号化して受信局に送信する。また、従来の受信局では、更新開始の通知を受けた第2の制御手段が以下の制御を行なう。受信した暗号化された新しい鍵を、復号鍵記憶手段75に記憶された既に暗号通信に使用してきた復号鍵を用いて第2の復号化手段76で復号化して新しい鍵を得る。

【0011】(E) 方式の場合、従来の送信局では、更新開始の通知を受けた第1の制御手段が以下の制御を行なう。第2の生成手段57で生成された新しい鍵を配達用暗号鍵記憶手段に記憶された配達用暗号鍵を用いて第2の暗号化手段59で暗号化して受信局に送信する。また、従来の受信局では、更新開始の通知を受けた第2の制御手段が以下の制御を行なう。受信した暗号化された新しい鍵を配達用復号鍵記憶手段76に記憶された配達用復号鍵を用いて第2の復号化手段76で復号化して新しい鍵を得る。

【0012】

【発明が解決しようとする課題】上記従来の暗号通信装置においては、暗号通信に用いる鍵を更新するときに、更新用の新しい鍵を、鍵更新前まで使用していた鍵で暗号化して配達するか、過去に使用された鍵で暗号化して配達するという手段を用いていた。しかし、配達に用いる鍵が既に一定期間使用した鍵なので、鍵の安全性が低いという問題を有していた。

【0013】また、別に用意した配達用の鍵で配達を行なう場合、暗号通信に使用する鍵とは別に、配達に使用する鍵を管理(生成・秘匿・更新)する必要が生じるという問題を有していた。

【0014】暗号通信のたびに更新を行なう場合、常に暗号通信時間に更新処理時間が加わるために、実際に暗

号通信が可能になるまでに時間がかかるという問題を有していた。

【0015】また、鍵の使用が任意の時間に達したときの場合、タイミングの変更を行なうために送信局-受信局間で任意の時間を決定するためのやりとりが必要となるので、同じタイミングで更新を行なうことが多くなり、解読を容易にする情報(鍵を暗号化した暗号文がどれであるか、どこまでの暗号文が同じ鍵で暗号化されているか等)が盗聴者に知られる可能性が高くなるという問題を有していた。

【0016】また、送信局または受信局から更新要求があったときの場合、ユーザーに更新判断が依存するためユーザーに負担となり、かつ更新判断の信頼性も低いという問題を有していた。

【0017】本発明は、上記従来の問題を解決するもので、定期的に更新される予備の鍵を常に用意することにより、使用時期をずらして、同じ鍵を暗号通信と配達に一定の安全性で使用できるようにしたものである。配達に使用する鍵は常に未使用なので安全性が高く、かつ配達用の鍵を管理(生成・更新)する手間を省くことができる優れた暗号通信装置を提供することを第1の目的とする。

【0018】また、受信局の配達鍵を暗号化しておくことにより、管理(秘匿)する手間を省くことができる優れた暗号通信装置を提供することを第2の目的とする。

【0019】また、予備鍵や平文に依存して更新のタイミングを決定することにより、更新のタイミングを変更するたびに送信局-受信局間でやりとりする必要が無く、かつ更新のタイミングがランダムになるので、上記の解読を容易にする情報が盗聴者に特定し難くなる優れた暗号通信装置を提供することを第3の目的とする。

【0020】

【課題を解決するための手段】本発明では、上記課題を解決するために、暗号通信装置の送信局においては、予備鍵を新規暗号鍵とし、生成手段により生成された予備鍵を新規予備鍵とし、予備鍵を暗号鍵で暗号化して送信し、その後、送信データを暗号鍵で暗号化して送信する構成とし、受信局においては、予備鍵を新規復号鍵とし、受信暗号化鍵を復号化して予備鍵とし、その後、受信暗号化データを復号化する構成とした。このように構成したことにより、予備の鍵を用意して常に未使用の鍵で新しい鍵を配達するので安全性が高くなり、同じ鍵を暗号通信と鍵配達に使用しても安全かつ簡便に暗号通信に使用する鍵を更新でき、かつ配達用の鍵を管理(生成・更新)する手間を省くことができる。

【0021】また、暗号通信装置の受信局において、受信暗号化鍵を暗号化予備鍵として記憶し、鍵更新の際に、暗号化予備鍵を復号化して新規復号鍵とする構成とした。このように構成したことにより、受信局において予備鍵を管理(秘匿)する手間を省くことができる。

【0022】また、暗号通信装置の送信局の判断手段で、送信回数と送信回数上限値を調べ、送信回数上限値が一定値以下ならば送信回数上限値に一定値の加算を行ない、送信回数と送信回数上限値が等しいならば更新情報を送信回数上限値へ書き込み、更新開始の通知を行ない、その後、新しい更新情報の更新情報記憶手段への転送を行なう構成とし、受信局の判断手段で、受信回数と受信回数上限値を調べ、受信回数上限値が一定値以下ならば受信回数上限値に一定値の加算を行ない、受信回数と受信回数上限値が等しいならば更新情報を受信回数上限値へ書き込み、更新開始の通知を行ない、その後、新しい更新情報の更新情報記憶手段への転送を行なう構成とした。このように構成したことにより、予備鍵や平文に依存して更新のタイミングを決定して、更新のタイミングを変更するたびに送信局-受信局間でやりとりする必要を無くし、かつ更新のタイミングがランダムになり、解読を容易にする情報を監聽者が特定し難くなる。

【0023】

【発明の実施の形態】本発明の請求項1に記載の発明は、送信局と受信局からなる暗号通信装置であって、前記送信局は、暗号鍵を記憶する暗号鍵記憶手段と、第1の予備鍵を記憶する第1の予備鍵記憶手段と、データを前記暗号鍵を用いて暗号化する第1の暗号化手段と、前記第1の予備鍵を前記暗号鍵を用いて暗号化する第2の暗号化手段と、前記第1の予備鍵を生成する生成手段と、前記第1の予備鍵を新規暗号鍵として前記暗号鍵記憶手段に転送し、前記生成手段により生成された予備鍵を新規第1の予備鍵として前記第1の予備鍵記憶手段に転送し、前記第2の暗号化手段の結果を出力し、その後前記第1の暗号化手段の結果を出力することを制御する第1の制御手段とを備え、前記受信局は、復号鍵を記憶する復号鍵記憶手段と、第2の予備鍵を記憶する第2の予備鍵記憶手段と、暗号化データを前記復号鍵を用いて復号化する第1の復号化手段と、前記第2の暗号化手段の結果を前記復号鍵を用いて復号化する第2の復号化手段と、前記第2の予備鍵を新規復号鍵として前記復号鍵記憶手段に転送し、前記第2の復号化手段の結果を新規第2の予備鍵として第2の予備鍵記憶手段に転送し、その後前記第1の復号化手段の結果を出力することを制御する第2の制御手段とを備える暗号通信装置であり、定期的に更新される予備の鍵を常に用意し、使用時期をずらして、同じ鍵を暗号通信と配送に一定の安全性で使用できるようにするという作用を有する。

【0024】本発明の請求項2に記載の発明は、請求項1記載の暗号通信装置において、送信局における前記第1の暗号化手段が、前記暗号鍵を用いて暗号化データを復号化し、受信局における前記第1の復号化手段が、前記復号鍵を用いてデータを暗号化するものであり、受信局から送信局に暗号化データを送ることを可能にすることによる作用を有する。

【0025】本発明の請求項3に記載の発明は、請求項1記載の暗号通信装置において、前記受信局が、復号鍵を記憶する復号鍵記憶手段と、前記第2の暗号化手段の結果を記憶する暗号化予備鍵記憶手段と、前記第1の暗号化手段の結果を前記復号鍵を用いて復号化する第1の復号化手段と、前記第2の暗号化手段の結果を前記復号鍵を用いて復号化する第2の復号化手段と、前記第2の暗号化手段の結果を暗号化予備鍵記憶手段に転送し、前記第2の復号化手段の結果を新規復号鍵として前記復号鍵記憶手段に転送することを制御する第2の制御手段とを備えるものであり、受信局の配送鍵を暗号化しておくことにより、管理（秘匿）する手間を省くという作用を有する。

【0026】本発明の請求項4に記載の発明は、請求項1記載の暗号通信装置において、前記送信局は、送信回数を計数する第1の計数手段と、前記送信回数と前記送信回数上限値を記憶する第1の回数記憶手段と、更新情報を記憶する第1の更新情報記憶手段と、前記送信回数と前記送信回数上限値を調べ、前記送信回数上限値が一定値以下ならば前記送信回数上限値に一定値の加算を行ない、前記送信回数と前記送信回数上限値が等しいならば前記更新情報を前記送信回数上限値へ書き込み、更新開始の通知を行ない、その後新規更新情報の前記更新情報記憶手段への転送を行なう第1の判断手段とを備え、前記受信局は、受信回数を計数する第2の計数手段と、前記受信回数と前記受信回数上限値を記憶する第2の回数記憶手段と、前記受信回数と前記受信回数上限値を調べ、前記受信回数上限値が一定値以下ならば前記受信回数上限値に一定値の加算を行ない、前記受信回数と前記受信回数上限値が等しいならば前記更新情報を前記受信回数上限値へ書き込み、更新開始の通知を行ない、その後新規更新情報の前記更新情報記憶手段への転送を行なう第2の判断手段とを備えるものであり、予備鍵や平文に応じて更新のタイミングを決定し、解読を容易にする情報を特定し難くするという作用を有する。

【0027】以下、本発明の実施の形態について、図1から図10を用いて詳細に説明する。

【0028】(第1の実施の形態)本発明の第1の実施の形態は、送信局において、予備鍵を暗号鍵で暗号化した結果を送信し、その後データを暗号鍵で暗号化した結果を送信し、受信局において、予備鍵記憶手段にある予備鍵を新規復号鍵として復号鍵記憶手段に転送し、受信暗号化予備鍵を復号鍵で復号した結果を予備鍵記憶手段に出力し、その後、受信暗号化データを復号鍵で復号した結果を出力する暗号通信装置である。

【0029】図1は、本発明の第1の実施の形態の暗号通信装置の送信局のブロック図である。図1において、点線で括られた範囲の各手段は、判断手段または制御手段により制御される。

【0030】図1において、入力端子10は、送信時に平

文データの入力を行なうものであり、コネクターで構成されている。

【0031】第1の計数手段11は、データの送信回数を計数するものであり、実際には、データの送信が行なわれるごとに、第1の回数記憶手段12に記憶された送信回数に1を加算するもので、ROMやRAMを内蔵したマイクロプロセッサ、例えばCPUやDSP等に計数アルゴリズムをプログラムした計数専用LSIとしたもので構成される。

【0032】第1の回数記憶手段12は、第1の計数手段11で計数された現在の送信回数と、鍵更新のタイミングを決定する送信回数上限値を記憶するメモリであり、例えばRAM等で構成される。

【0033】第1の判断手段13は、第1の回数記憶手段12に記憶されたデータの送信回数が一定の回数以上に達したか判定するとともに、送信回数上限値を更新するものであり、実際には、第1の回数記憶手段12に記憶されている現在の送信回数と送信回数上限値を比較し、等しければ第1の更新情報記憶手段14に記憶されている更新情報を第1の回数記憶手段12に転送し、第1の制御手段18に更新開始を通知し、新規更新情報を第1の更新情報記憶手段14に転送する操作と、第1の回数記憶手段12の送信回数上限値が予め設定した数以下ならば一定値を加算する操作を行なうもので、ROMやRAMを内蔵したマイクロプロセッサ、例えばCPU、DSP等に判断アルゴリズムをプログラムした判断専用LSIとしたもので構成される。送信回数上限値の更新は、第1の更新情報記憶手段14から転送されてくる更新情報を、第1の回数記憶手段12の送信回数上限値に上書きすることで行なう。ただし、送信回数上限値が0回では更新ばかり行なわれ、暗号通信状態に移行しないという問題が生じる。また、頻繁に一桁の回数で更新が行なわれると処理時間が増加して運用に支障をきたす。この問題を回避するために、送信回数上限値が0回や一桁の回数のときには、一定値を加算する操作を行なう。また、送信回数上限値の有効範囲と加算値は、実際の通信頻度により決定するべきである。更新情報としては予備鍵や平文を用いることが考えられる。予備鍵の場合には、第1の生成手段15で生成された予備鍵の特定の位置（例えば先頭または後尾）から一定数のビットを、第1の更新情報記憶手段14に転送する。平文の場合には、鍵更新後に最初に暗号化して送信する平文の特定の位置（例えば先頭または後尾）から一定数のビットを更新情報記憶手段に転送する。また、転送する更新情報を何ビットにするかで、鍵更新の期間を一定範囲に決定することができ、例えば8ビットにすれば0～255回の範囲に決定することができる。

【0034】第1の更新情報記憶手段14は、更新情報を記憶するメモリであり、例えばRAM等で構成される。

【0035】生成手段15は、予備鍵（疑似乱数）を生成

するものであり、ROMやRAMを内蔵したマイクロプロセッサ、例えばCPU・DSP等に生成アルゴリズムをプログラムした生成専用LSIとしたもので構成される。乱数生成アルゴリズムとしては、LFSR (Linear Feedback Shift Registers) を用いるのが一般的である。しかし、兼用が可能であれば暗号アルゴリズムやハッシュアルゴリズムを用いることもある。また、疑似乱数生成にはシードと呼ばれる初期値が必要であり、例えばCPU・DSP等のシステムクロックをシードとして利用することができる。

【0036】第1の予備鍵記憶手段16は、第1の生成手段15で生成された予備鍵を記憶するメモリであり、例えばRAM等で構成される。

【0037】暗号鍵記憶手段17は、第1の暗号化手段19と第2の暗号化手段20で暗号化に用いる暗号鍵を記憶するメモリであり、例えばRAM等で構成される。

【0038】第1の制御手段18は、更新開始の通知を受けると、以下の動作を順番に行なうように制御するものであり、ROMやRAMを内蔵したマイクロプロセッサ、例えばCPU・DSP等に制御アルゴリズムをプログラムした制御専用LSIとしたもので構成される。初めに、第1の予備鍵記憶手段16に予め記憶されている予備鍵を暗号鍵記憶手段17に転送し、次に生成手段15に予備鍵の生成を指示し、次にこの生成された予備鍵を新規予備鍵として第1予備鍵記憶手段16と第2の暗号化手段20に転送し、次にこの予備鍵の暗号化を第2の暗号化手段20に指示し、最後にこの暗号化暗号鍵を受信局に送信する。

【0039】第1の暗号化手段19は、暗号鍵記憶手段17に記憶されている暗号鍵を用いてデータを暗号化するものであり、ROMやRAMを内蔵したマイクロプロセッサ、例えばCPU・DSP等に暗号アルゴリズムをプログラムした暗号専用LSIとしたもので構成される。しかし、ROMやRAMを内蔵したマイクロプロセッサ、例えばCPU・DSP等に暗号アルゴリズムをプログラムするのが面倒であれば、初めから暗号専用のLSIとして開発され市販されているものを使用することもできる。また、本発明では暗号として共通（秘密）鍵ブロック暗号を用いており、その種類としてDES・FEAL・IDEA等が挙げられるが、どの暗号を用いても本発明は有効であると考えられる。

【0040】第2の暗号化手段20は、暗号鍵記憶手段17に記憶されている暗号鍵を用いて鍵を暗号化するものであり、第1の暗号化手段と同じものである。

【0041】出力端子21は、送信時には暗号化データの出力を行ない、受信時には平文データの出力を行なうものであり、コネクター等で構成されている。

【0042】図2は、本発明の第1の実施の形態の暗号通信装置の受信局のブロック図である。図2において、点線で括られた範囲の各手段は、判断手段または制御手

段により制御される。図2において、入力端子30は、受信時に暗号化データの入力を行なうものであり、コネクターで構成されている。

【0043】第2の計数手段31は、データの受信回数を計数するものであり、実際にはデータの受信が行なわれるごとに、第2の回数記憶手段32に記憶された受信回数に1を加算するもので、ROMやRAMを内蔵したマイクロプロセッサ、例えばCPUやDSP等に計数アルゴリズムをプログラムした計数専用LSIとしたもので構成される。

【0044】第2の回数記憶手段32は、第2の計数手段31で計数された現在の受信回数と鍵更新のタイミングを決定する受信回数上限値を記憶するメモリであり、例えばRAM等で構成される。

【0045】第2の判断手段33は、第2の回数記憶手段32に記憶されたデータの受信回数が一定の回数以上に達したか判定するとともに、受信回数上限値を更新するものであり、実際には、回数記憶手段32に記憶されている現在の受信回数と、予め設定されている受信回数上限値を比較し、等しければ第2の更新情報記憶手段34に記憶されている更新情報を第2の回数記憶手段32に転送し、第2の制御手段37に更新開始を通知し、新規更新情報を更新情報記憶手段34に転送する操作と、第2の回数記憶手段32の受信回数上限値が予め設定した数以下ならば一定値を加算する操作を行なうもので、ROMやRAMを内蔵したマイクロプロセッサ、例えばCPU・DSP等に判断アルゴリズムをプログラムした判断専用LSIとしたもので構成される。受信回数上限値の更新は、第2の更新情報記憶手段34から転送されてくる更新情報を第2の回数記憶手段32の受信回数上限値に上書きすることで行なう。ただし、受信回数上限値が0回では更新ばかり行なわれ暗号通信状態に移行しないという問題が生じる。また、頻繁に一桁の回数で更新が行なわれると処理時間が増加して運用に支障をきたす。この問題を回避するために、受信回数上限値が0回や一桁の回数のときは一定値を加算する操作を行なう。また、受信回数上限値の有効範囲と加算値は、実際の通信頻度により決定するべきである。更新情報としては予備鍵や平文を用いることが考えられる。予備鍵を用いるには、第2の復号化手段38で復号化された予備鍵の特定の位置（例えば先頭または後尾）から一定数のビットを第2の更新情報記憶手段に転送する。平文の場合には、鍵更新後に最初に受信して第1の復号化手段39で復号化した平文の特定の位置（例えば先頭または後尾）から一定数のビットを第2の更新情報記憶手段34に転送する。また、転送する更新情報を何ビットにするかで鍵更新の期間を一定範囲に決定することができ、例えば8ビットにすれば0～255回の範囲に決定できる。

【0046】第2の更新情報記憶手段34は、更新情報を記憶するメモリであり、例えばRAM等で構成される。

【0047】第2の予備鍵記憶手段35は、予備鍵を記憶するメモリであり、例えばRAM等で構成される。

【0048】復号鍵記憶手段36は、復号鍵を記憶するメモリであり、例えばRAM等で構成される。

【0049】第2の制御手段37は、更新開始の通知を受けると、以下の動作を順番に行なうように制御するものであり、ROMやRAMを内蔵したマイクロプロセッサ、例えばCPU・DSP等に制御アルゴリズムをプログラムした制御専用LSIとしたもので構成される。初めに、第2の予備鍵記憶手段35に予め記憶されている予備鍵を新規復号鍵として復号鍵記憶手段36に転送し、次に受信した暗号化予備鍵を第2の復号化手段38に転送し、次に第2の復号化手段38に前記暗号化予備鍵の復号化を指示し、最後に復号化された予備鍵を新規予備鍵として第2の予備鍵記憶手段に転送する。

【0050】第1の復号化手段38は、復号鍵記憶手段36に記憶された復号鍵を用いてデータを復号化するものであり、ROMやRAMを内蔵したマイクロプロセッサ、例えばCPU・DSP等に暗号アルゴリズムをプログラムした暗号専用LSIとしたもので構成される。しかし、ROMやRAMを内蔵したマイクロプロセッサ、例えばCPU・DSP等に暗号アルゴリズムをプログラムするのが面倒であれば、送信局と同様に初めから暗号専用のLSIとして開発されたものを使用することもできる。また、本発明では暗号として共通（秘密）鍵ブロック暗号を用いており、その種類としてDES・FEAL・IDEA等が挙げられるが、どの暗号を用いても本発明は有効であると考えられる。

【0051】第2の復号化手段39は、復号鍵記憶手段36に記憶された復号鍵を用いて鍵を復号化するものであり、第1の復号化手段と同じものである。

【0052】出力端子40は、受信時にデータの出力を行なうものであり、コネクターで構成されている。

【0053】以上のように構成された暗号通信装置について、図3と図4を用いて、その動作を説明する。ここで図3が送信局の動作、図4が端末機の動作を示す。図3について説明する。

【0054】初めに、入力として受信局へ送信する通信文（平文）を考える。ステップ1～4までが鍵更新プロセスへの移行を判断するプロセスである。

【0055】ステップ1・2では、第1の計数手段11が入力として送信データが送られて来たことを確認し、第1の回数記憶手段12に記憶されている送信回数に1を加算する。

【0056】ステップ3では、第1の回数記憶手段12に記憶されている送信回数上限値が以下であれば上限値に一定値を加算する。

【0057】ステップ4では、第1の回数記憶手段12に記憶されている送信回数と送信回数の上限Mを比較し、等しければ第1の制御手段13に更新開始を通知し、そ

でなければステップ1に戻る。ステップ5以降の動作は全て第1の制御手段13により順番に実行される鍵更新プロセスである。

【0058】ステップ5では、第1の更新情報記憶手段14に記憶されている更新情報を第1の回数記憶手段12の送信回数上限値に上書きする。

【0059】ステップ6では、第1の予備鍵記憶手段16に記憶されている予備鍵を新規暗号鍵として暗号鍵記憶手段17に転送する。

【0060】ステップ7では、生成手段15で予備鍵(疑似乱数)を生成する。

【0061】ステップ8では、ステップ7で生成された予備鍵を新規予備鍵として第1の予備鍵記憶手段16と第2の暗号化手段20に転送する。

【0062】ステップ9では、ステップ8で第2の暗号化手段20に転送された予備鍵を暗号鍵記憶手段17に記憶されている暗号鍵で暗号化する。

【0063】ステップ10では、ステップ9で生成された暗号化予備鍵を受信局に送信する。ステップ11では、新規更新情報を第1の更新情報記憶手段14に転送する。ステップ11終了後、出力として更新された暗号鍵を用いて通信文(入力平文)を暗号化して出力する。

【0064】図4について説明する。ステップ1~4までが鍵更新プロセスへの移行を判断するプロセスである。

【0065】ステップ1・2では、第2の計数手段31が入力として受信データが送られて来たことを確認し、第2の回数記憶手段32に記憶されている受信回数に1を加算する。

【0066】ステップ3では、第2の判断手段33が第2の回数記憶手段32に記憶されている受信回数上限値がJ以下であれば上限値に一定値を加算する。

【0067】ステップ4では、第2の回数記憶手段32に記憶されている受信回数上限値が第2の回数記憶手段32に記憶されている受信回数と受信回数の上限Mを比較し、等しければ第2の制御手段33に更新開始を通知し、そうでなければステップ1に戻る。ステップ5以降の動作は全て第2の制御手段37により順番に実行される鍵更新プロセスである。

【0068】ステップ5では、第2の更新情報記憶手段34に記憶されている更新情報を第2の回数記憶手段32の受信回数上限値に書き込む。

【0069】ステップ6では、第2の予備鍵記憶手段35に記憶された予備鍵を復号鍵記憶手段36に転送する。

【0070】ステップ7では、受信した暗号化予備鍵を第2の復号化手段39に転送する。

【0071】ステップ8では、ステップ7で転送した暗号化予備鍵を第2の復号化手段39で復号鍵記憶手段36に記憶された復号鍵を用いて復号化する。

【0072】ステップ9では、ステップ8で復号化され

た予備鍵を新規復号鍵として第2の予備鍵記憶手段35に転送する。

【0073】ステップXは、新規更新情報が平文か予備鍵かで実行されるタイミングが異なる。予備鍵であれば、予備鍵が復号化されるステップ8終了後に実行される。平文の場合には、鍵更新終了後に最初に受信した暗号文を復号化して得られる平文を入手した後に実行される。

【0074】図5は、送信局と受信局を接続した暗号通信装置全体の構成について示したものである。本発明では、送信局の入出力端子21と受信局の入出力端子30の接続は有線を想定しており、ケーブル、例えば同軸ケーブルで構成される。また、本発明の鍵更新装置は無線通信システムにも使用可能であると考えられる。図5では、説明の簡略化のために受信局は1台しか示していないが、実際には複数の受信局を想定している。これは送信局が基地局で、受信局が端末局のような場合も考えているからである。受信局が複数の場合にも受信局側はこれまでの説明と同様である。しかし、送信局は受信局の台数だけ鍵更新を行なう必要があるので、鍵と送信回数と送信回数上限値を受信局ごとに分けて記憶しなければならない。つまり、送信局の第1の回数記憶手段と第1の予備鍵記憶手段と第1の暗号鍵記憶手段にはそれぞれ受信局ごとの送信回数と送信回数上限値と予備鍵と暗号鍵を記憶しておく。

【0075】実装上の留意点としては、送信局の第1の計数手段11、第1の判断手段13、第1の制御手段18、生成手段15、第1の暗号化手段19、第2の暗号化手段20を個々にマイクロプロセッサーを用いて構成すると効率が悪いので、性能に問題がなければ一つのマイクロプロセッサーで兼用するのが望ましい。また、受信局についても同様に第2の計数手段31、第2の判断手段33、第2の制御手段37、第1の復号化手段38、第2の復号化手段39を一つのマイクロプロセッサーで兼用するのが望ましい。

【0076】図6と図7は、各通信状態における鍵の配置を示したもので、横方向が通信状態、縦方向が鍵の状態を表す。

【0077】図6に示す送信局の場合は以下のように鍵の状態が推移する。

【0078】状態:1は、通信を行なう前の準備段階であり、初めに鍵Aと鍵Bをセットする。また、このとき同時に鍵を更新する送信回数および受信回数の上限値の初期値を送信局と受信局の間で決定しておく。

【0079】状態:2は、最初の暗号通信状態であり、暗号鍵記憶手段の暗号鍵Aで暗号通信を行ない、第1の予備鍵記憶手段16の予備鍵Bは使用しない。送信回数が一定値に達した時点で状態:3へ移行する。

【0080】状態:3は、最初の鍵更新状態であり、第1の予備鍵記憶手段16の予備鍵Bを新規暗号鍵として暗

号鍵記憶手段17に転送して暗号鍵Bとする。これにより暗号鍵Aは廃棄されることになる。次に鍵Cを生成し、第1の予備鍵記憶手段16に新規予備鍵として転送する。最後に予備鍵Cを暗号鍵Bで暗号化して送信し、状態: 4に移行する。

【0081】状態: 4は、暗号通信状態であり、暗号鍵記憶手段17の暗号鍵Bで暗号通信を行ない、第1の予備鍵記憶手段16の予備鍵Cは使用しない。送信回数上限値が一定値に達した時点で状態: 5へ移行する。

【0082】状態: 5は鍵更新状態であり、第1の予備鍵記憶手段16の予備鍵Cを新規暗号鍵として暗号鍵記憶手段17に転送して暗号鍵Cとする。これにより暗号鍵Bは廃棄されることになる。次に鍵Dを生成し、第1の予備鍵記憶手段16に新規予備鍵として転送する。最後に予備鍵Dを暗号鍵Cで暗号化して送信し、状態: 6に移行する。

【0083】状態: 6は、暗号通信状態であり、暗号鍵記憶手段17の暗号鍵Cで暗号通信を行ない、第1の予備鍵記憶手段16の予備鍵Dは使用しない。以下、鍵配達状態と暗号通信状態が交互に繰り返される。

【0084】図7に示す受信局の場合は、以下のように鍵の状態が推移する。

【0085】状態: 1は、通信を行なう前の準備段階であり、初めに鍵Aと鍵Bをセットしておく。また、このとき同時に鍵を更新する送信回数および受信回数の上限値の初期値を送信局と受信局の間で決定しておく。

【0086】状態: 2は、最初の暗号通信状態であり、復号鍵記憶手段36の復号鍵Aで暗号通信を行ない、第2の予備鍵記憶手段35の予備鍵Bは使用せず、受信回数が一定値に達した時点で状態: 3へ移行する。

【0087】状態: 3は、最初の鍵更新状態であり、第2の予備鍵記憶手段35の予備鍵Bを新規復号鍵として復号鍵記憶手段36に転送して復号鍵Bとする。よって、復号鍵Aは廃棄されることになる。次に暗号化Cを受信し、復号鍵Bで復号化して新規予備鍵として第2の予備鍵記憶手段35に転送する。鍵更新終了後、状態: 4に移行する。

【0088】状態: 4は、暗号通信状態であり、復号鍵記憶手段36の復号鍵Bで暗号通信を行ない、第2の予備鍵記憶手段35の予備鍵Cは使用しない。受信回数が一定値に達した時点で、状態: 5へ移行する。

【0089】状態: 5は、鍵更新状態であり、第2の予備鍵記憶手段35の予備鍵Cを新規復号鍵として復号鍵記憶手段36に転送して復号鍵Cとする。よって、復号鍵Bは廃棄されることになる。次に暗号化Dを受信し、復号鍵Cで復号化して新規予備鍵として第2の予備鍵記憶手段35に転送する。鍵更新終了後、状態: 6に移行する。

【0090】状態: 6は、暗号通信状態であり、復号鍵記憶手段36の復号鍵Cで暗号通信を行ない、第2の予備鍵記憶手段35の予備鍵Dは使用しない。以下、鍵配達状態と暗号通信状態が交互に繰り返される。

【0091】最後に、従来の暗号通信装置と本発明の鍵の更新による安全性が全体としてみたときにはどのように考えられるかを説明する。本発明では、使用時間をずらすことにより暗号用の鍵と配達用の鍵を一つの鍵で共有している。この方法は配達用の鍵に暗号通信に未使用の鍵を用いているので、配達用の鍵を用意しない場合よりは安全性が高い。ただし、盗聴者が暗号用の鍵を解読でき、かつ以前に配達された予備鍵を暗号化した暗号文を保持していると、別に配達用の鍵を用意する場合より安全性が低くなる場合がある。しかし、鍵の更新のタイミングをランダムにすることにより、予備鍵を暗号化した暗号文を特定し難くしてある。したがって、別に配達用の鍵を用意する場合において同じ配達鍵を使い続ければ、本発明の安全性の方が高くなっていく可能性が高い。

【0092】上記のように、本発明の第1の実施の形態では、暗号通信装置を、送信局において、予備鍵を暗号鍵で暗号化した結果を送信し、その後データを暗号鍵で暗号化した結果を送信し、受信局において、予備鍵記憶手段にある予備鍵を新規復号鍵として復号鍵記憶手段に転送し、受信暗号化予備鍵を復号鍵で復号した結果を予備鍵記憶手段に出力し、その後、受信暗号化データを復号鍵で復号した結果を出力する構成としたので、未使用の鍵で予備鍵を配達するので、鍵配達の安全性が高くなる。

【0093】(第2の実施の形態) 本発明の第2の実施の形態は、受信局において、受信暗号化予備鍵を暗号化予備鍵記憶手段に転送し、鍵更新の際に、暗号化予備鍵記憶手段の暗号化予備鍵を復号鍵で復号した結果を新規復号鍵として復号鍵記憶手段に転送する暗号通信装置である。

【0094】第2の実施の形態の暗号通信装置が、第1の実施の形態と異なるところは、予備鍵を受信側で暗号化予備鍵のままで記憶しておき、復号鍵として使用する直前に復号する点である。

【0095】図8は、本発明の第2の実施の形態の暗号通信装置の受信局のブロック図である。図8において、入力端子30、第2の計数手段31、第2の回数記憶手段32、第2の判断手段33、第2の更新情報記憶手段34、復号鍵記憶手段36、第1の復号化手段38、第2の復号化手段39、出力端子40は、第1の実施の形態と同じである。

【0096】暗号化予備鍵記憶手段35は、受信した暗号化予備鍵を記憶するメモリである。

【0097】第2の制御手段37は、更新開始の通知を受けると、以下の動作を順番に行なうように制御するものである。初めに、暗号化予備鍵記憶手段35の暗号化予備鍵を第2の復号化手段38に転送し、次に前記暗号化予備鍵の復号化を第2の復号化手段38に指示し、次に復号化された予備鍵を新規復号鍵として復号鍵記憶手段36に転

送し、最後に受信した暗号化予備鍵を新規暗号化予備鍵として暗号化予備鍵記憶手段に転送する。

【0098】以上のように構成された暗号通信装置について、図9に示す受信局のフローチャートを用いて受信局の動作を説明する。送信局の動作は第1の実施の形態と同じである。ステップ1～5までのプロセスは、第1の実施の形態と同じである。

【0099】ステップ6では、暗号化予備鍵記憶手段35'に記憶されている暗号化予備鍵を第2の復号化手段39に転送する。

【0100】ステップ7では、ステップ6で転送した暗号化予備鍵を第2の復号化手段39で復号鍵記憶手段36に記憶された復号鍵を用いて復号する。

【0101】ステップ8では、ステップ7で復号化された予備鍵を新規復号鍵として復号鍵記憶手段36に転送する。

【0102】ステップ9では、受信した暗号化予備鍵を新規暗号化予備鍵として暗号化予備鍵記憶手段35'に転送する。

【0103】ステップXは、新規更新情報が平文か予備鍵かで実行されるタイミングが異なる。予備鍵であれば、予備鍵が復号化されるステップ8終了後に実行される。平文の場合には、鍵更新終了後に最初に受信した暗号文を復号化して得られる平文を入手した後に実行される。

【0104】図10は、受信局の各通信状態における鍵の配置を示したもので、横方向が通信状態、縦方向が鍵の状態を表す。以下のように鍵の状態が推移する。

【0105】状態:1は、通信を行なう前の準備段階であり、初めに鍵Aと、鍵Bを鍵Aで暗号化した暗号化Bをセットしておく。また、このとき同時に鍵を更新する送信回数および受信回数の上限値の初期値を送信局と受信局の間で決定しておく。

【0106】状態:2は、最初の暗号通信状態であり、復号鍵記憶手段36の復号鍵Aで暗号通信を行ない、暗号化予備鍵記憶手段35'の暗号化Bは使用しない。受信回数が一定値に達した時点で状態:3へ移行する。

【0107】状態:3は、最初の鍵更新状態であり、暗号化予備鍵記憶手段35'の暗号化Bを復号鍵Aで復号化して復号鍵記憶手段36に転送する。よって、復号鍵Aは廃棄されることになる。次に暗号化Cを受信し、暗号化予備鍵記憶手段35'に新規暗号化予備鍵として転送する。鍵更新終了後、状態:4に移行する。

【0108】状態:4は、暗号通信状態であり、復号鍵記憶手段36の復号鍵Bで暗号通信を行ない、暗号化予備鍵記憶手段35'の暗号化Cは使用しない。受信回数が一定値に達した時点で状態:5へ移行する。

【0109】状態:5は、鍵更新状態であり、暗号化予備鍵記憶手段35'の暗号化Cを復号鍵Bで復号化して復号鍵記憶手段36に転送する。よって、復号鍵Bは廃棄さ

れたことになる。次に暗号化Dを受信し、暗号化予備鍵記憶手段35'に新規暗号化予備鍵として転送する。鍵更新終了後、状態:6に移行する。

【0110】状態:6は、暗号通信状態であり、復号鍵記憶手段36の復号鍵Cで暗号通信を行ない、暗号化予備鍵記憶手段35'の暗号化Dは使用しない。以下、鍵配達状態と暗号通信状態が交互に繰り返される。

【0111】上記のように、本発明の第2の実施の形態では、暗号通信装置を、受信局において、受信暗号化予備鍵を暗号化予備鍵記憶手段に転送し、鍵更新の際に、暗号化予備鍵記憶手段の暗号化予備鍵を復号鍵で復号した結果を新規復号鍵として復号鍵記憶手段に転送する構成としたので、鍵を暗号化した状態で保存でき、配送鍵の管理（秘匿）を行なう手段を別途設ける必要が無くなる。

【0112】なお、第1および第2の実施の形態では、送信局で送信し、受信局で受信する動作を説明したが、受信局の復号鍵を使って暗号化し、送信局の暗号鍵を使って復号化することもできる。

【0113】

【発明の効果】以上のように、本発明によれば、暗号通信装置を、鍵配達ごとに更新される予備鍵を用意し、この予備鍵を用いて、制御手段は配達用の鍵が常に暗号通信に未使用の暗号鍵になるように転送順序を制御する構成としたので、未使用の鍵で配達する分だけ安全性が高くなるという効果が得られる。

【0114】また、本発明では、一つの鍵を鍵配達と暗号通信に一定の安全性で使用できるので、別に配送鍵の管理（生成・更新）を行なう必要が無くなるという効果が得られる。

【0115】また、本発明では、鍵を暗号化した状態で保存できるので、別に配送鍵の管理（秘匿）を行なう必要が無くなるという効果が得られる。

【0116】また、本発明では、送信または受信回数をタイミングとして計数手段により計数し、判断手段が一定回数に達したことを通知することにより、定期的に鍵更新を行なう構成としたので、処理が軽くなるとともに、自動で鍵更新が行なわれて、ユーザーに負担がかかるなくなるという効果が得られる。

【0117】また、本発明では、判断手段により更新情報に依存して鍵の更新のたびにタイミングを更新するので、情報が盗聴者に知られる可能性が低くなるという効果が得られる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態における送信局の構成を示すブロック図、

【図2】本発明の第1の実施の形態における受信局の構成を示すブロック図、

【図3】本発明の第1の実施の形態における送信局の鍵更新の動作フロー図、

【図4】本発明の第1の実施の形態における受信局の鍵更新の動作フロー図、

【図5】本発明の第1の実施の形態における暗号通信装置の構成を示すブロック図、

【図6】本発明の第1の実施の形態における送信局における鍵の状態のタイミング図、

【図7】本発明の第1の実施の形態における受信局における鍵の状態のタイミング図、

【図8】本発明の第2の実施の形態における受信局の構成を示すブロック図、

【図9】本発明の第2の実施の形態における受信局の鍵更新の動作フロー図、

【図10】本発明の第2の実施の形態における受信局における鍵の状態のタイミング図、

【図11】従来の暗号通信装置における送信局の構成を示すブロック図、

【図12】従来の暗号通信装置における受信局の構成を示すブロック図である。

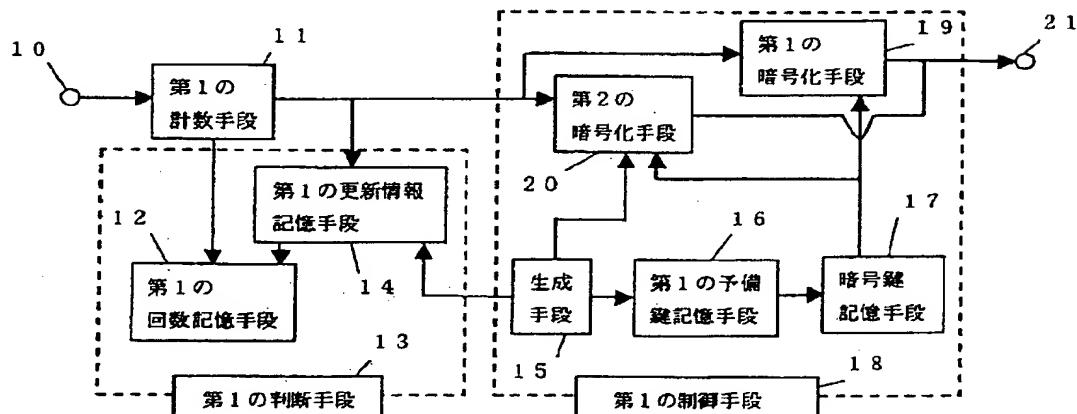
【符号の説明】

11 第1の計数手段

- 12 第1の回数記憶手段
- 13 第1の判断手段
- 14 第1の更新情報記憶手段
- 15 生成手段
- 16 第1の予備鍵記憶手段
- 17 暗号鍵記憶手段
- 18 第1の制御手段
- 19 第1の暗号化手段
- 20 第2の暗号化手段
- 31 第2の計数手段
- 32 第2の回数記憶手段
- 33 第2の判断手段
- 34 第2の更新情報記憶手段
- 35 第2の予備鍵記憶手段
- 35' 暗号化予備鍵記憶手段
- 36 復号鍵記憶手段
- 37 第2の制御手段
- 38 第1の復号化手段
- 39 第2の復号化手段

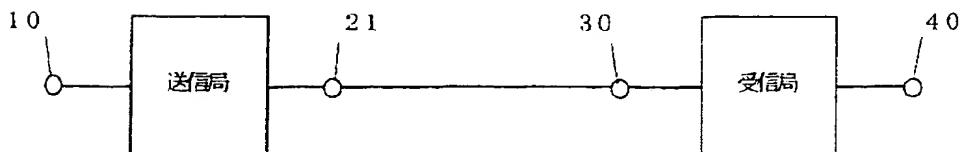
【図1】

送信局



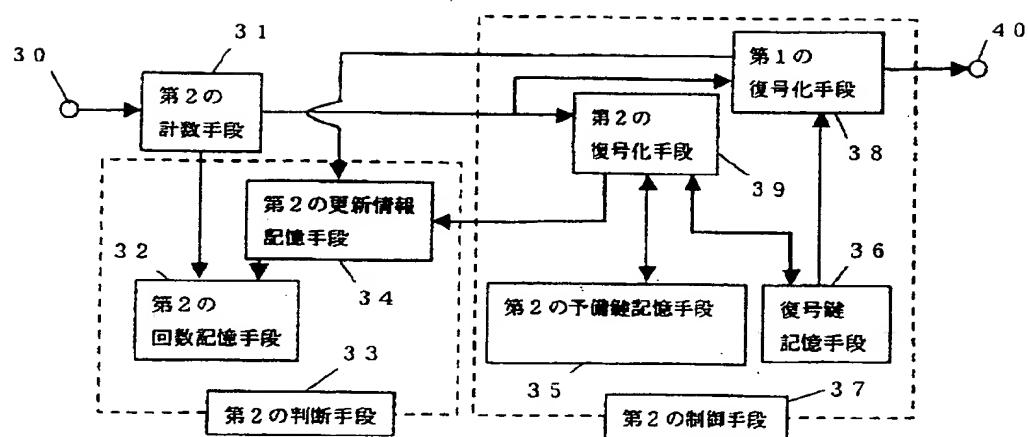
【図5】

暗号通信装置全体



[図2]

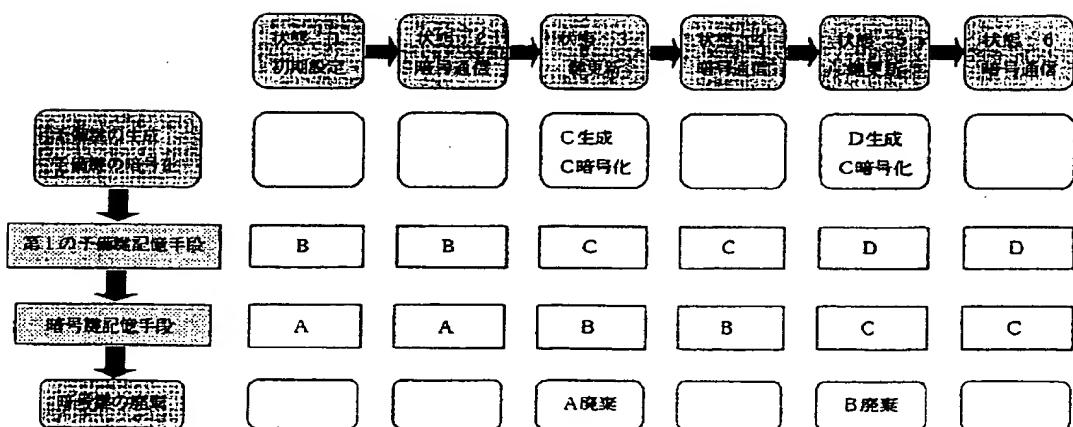
受信局



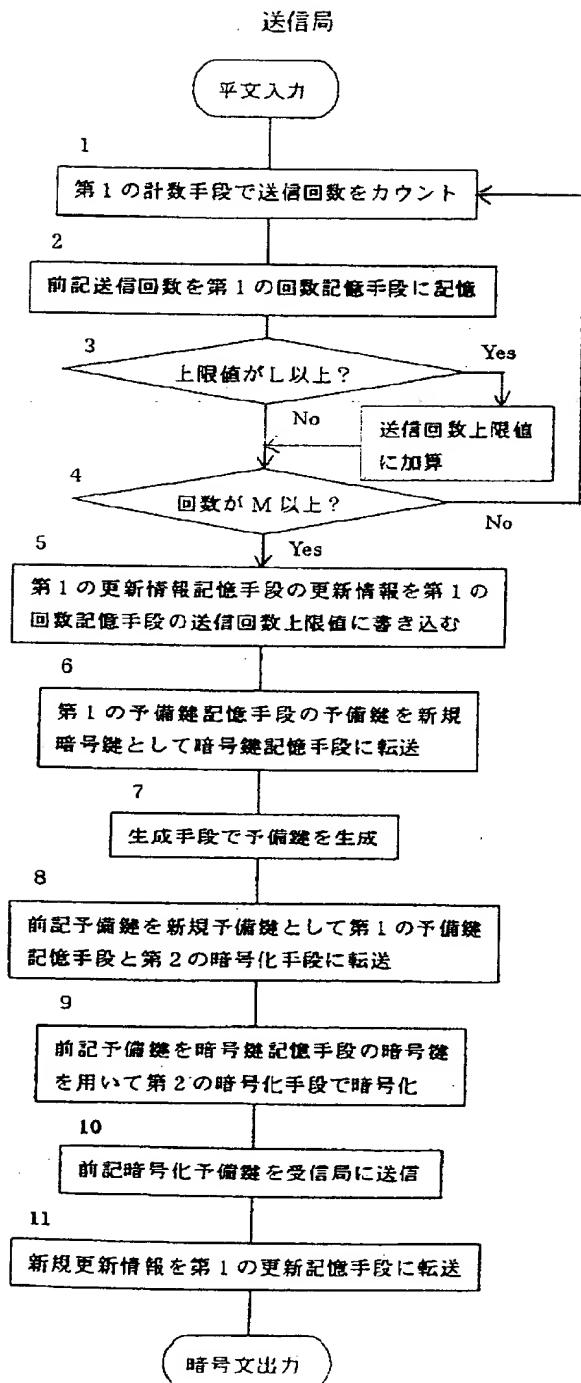
[图 6]

鍵の状態

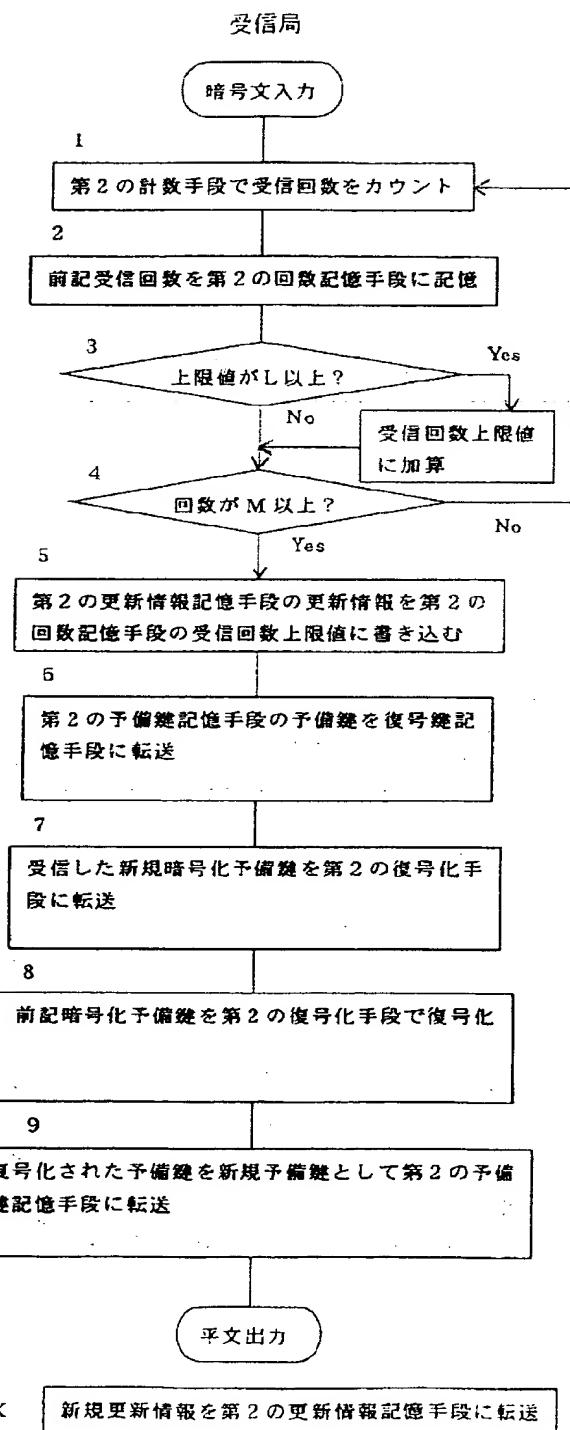
送信局



【図3】

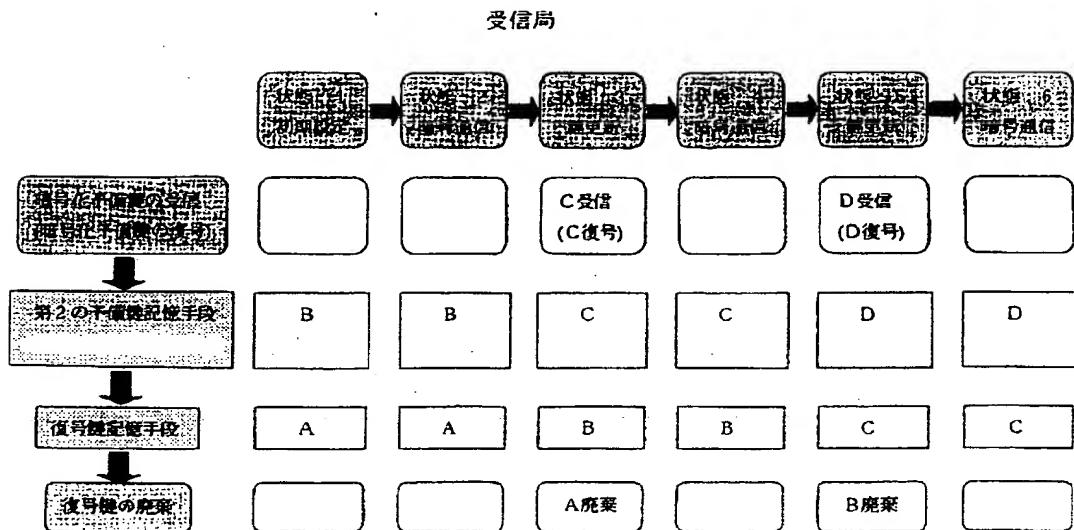


【図4】

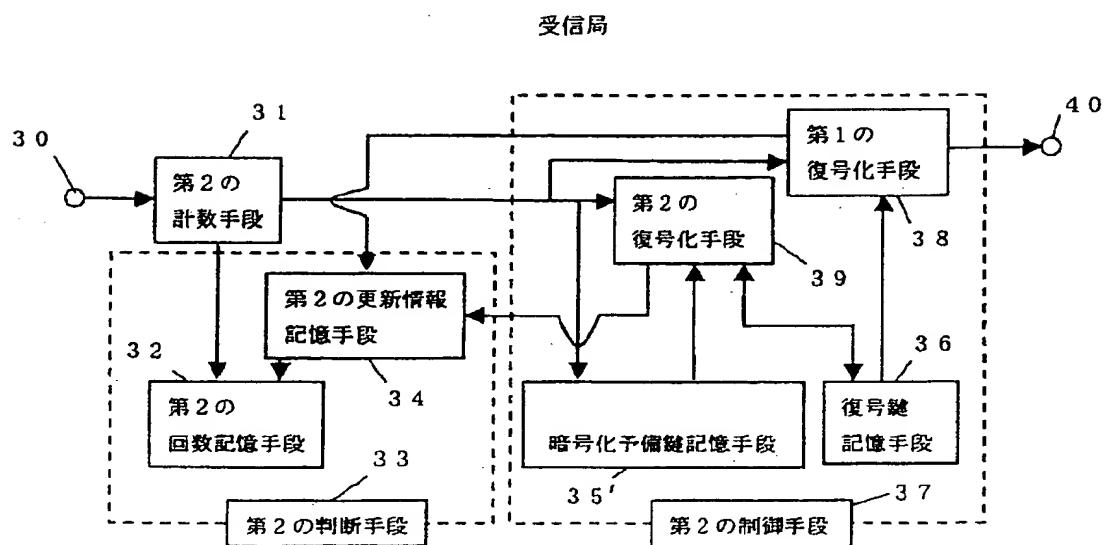


※2 Xは更新情報の種類によりタイミングが異なる。

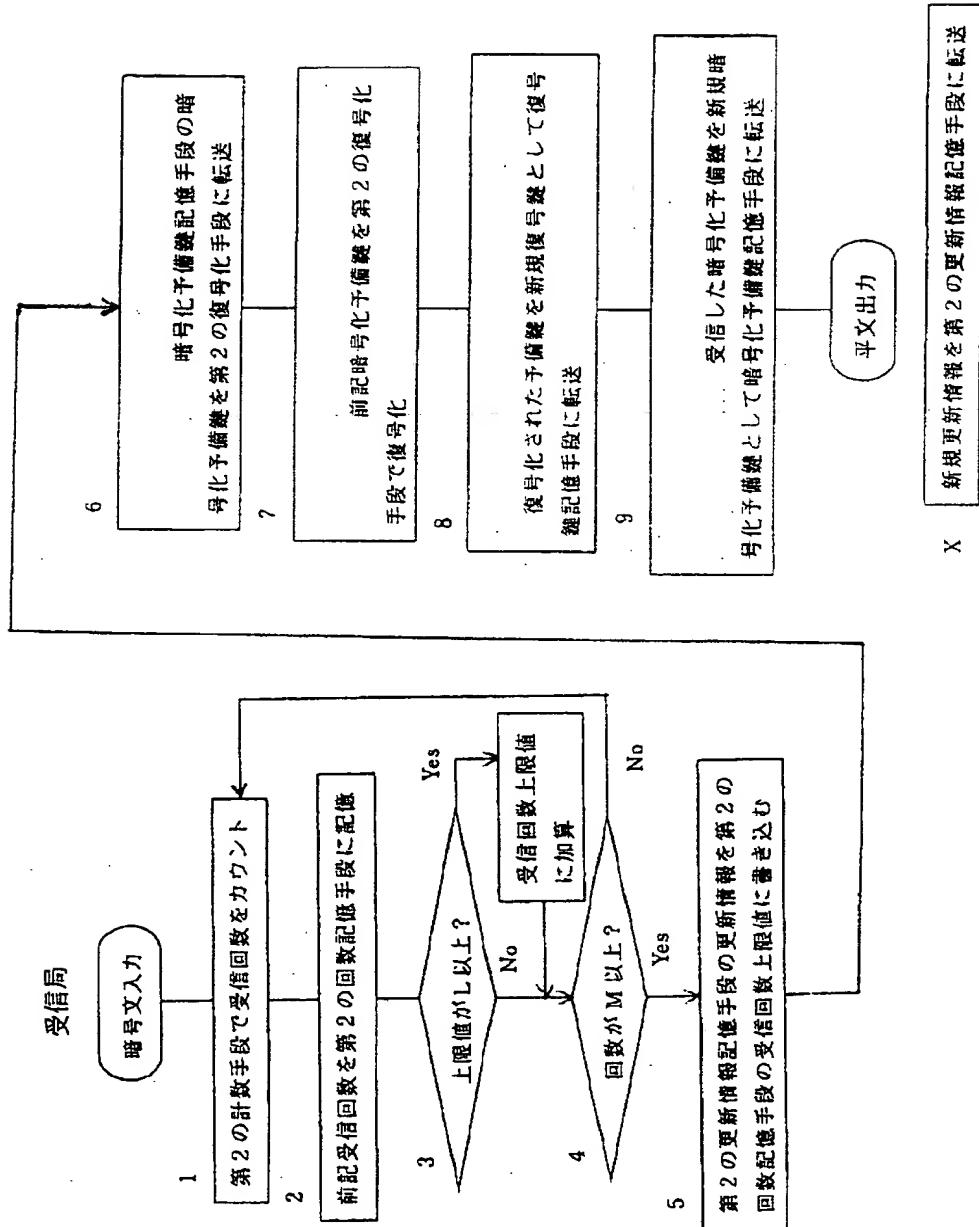
【図7】



【図8】

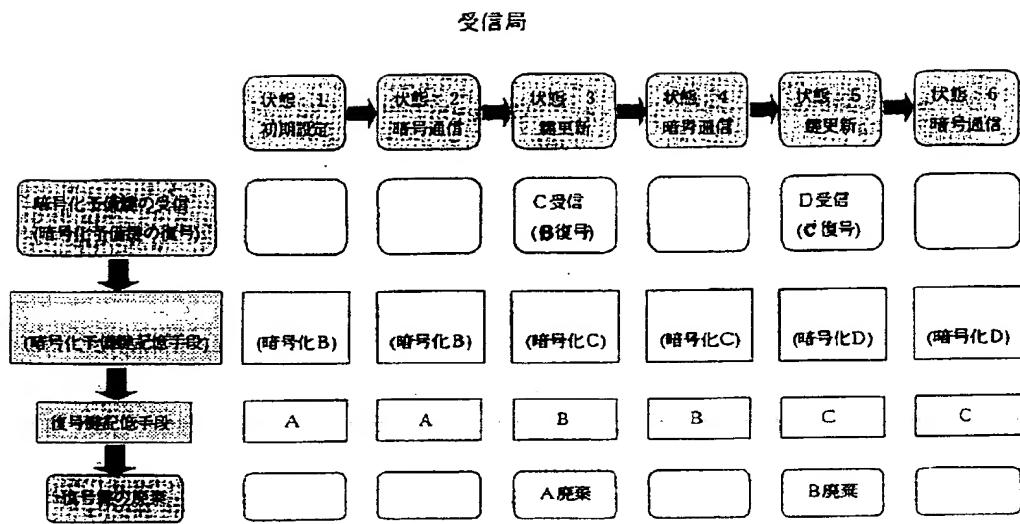


【図9】

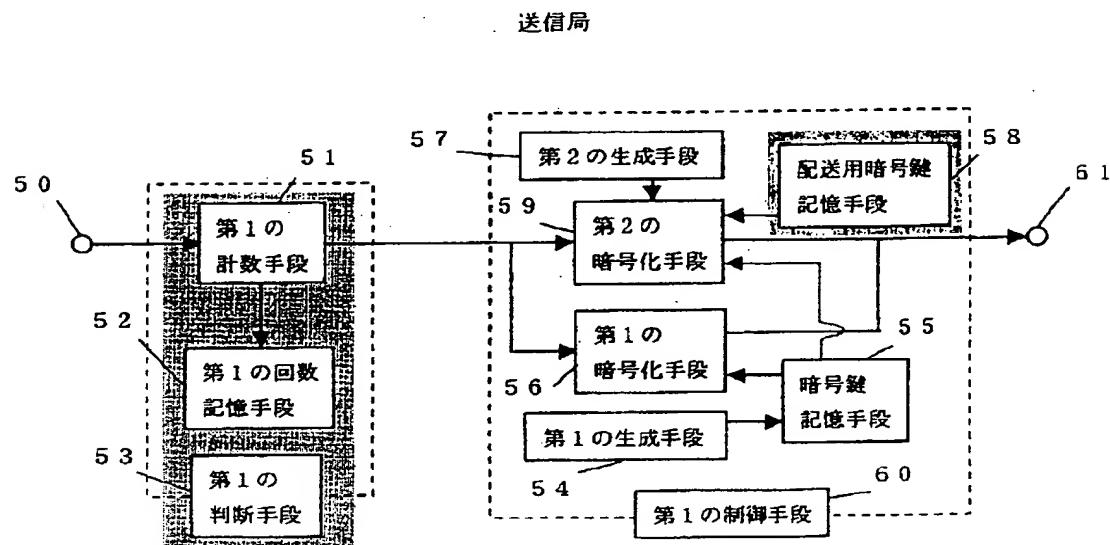


※2 Xは更新情報の種類によりタイミングが異なる。

【図10】

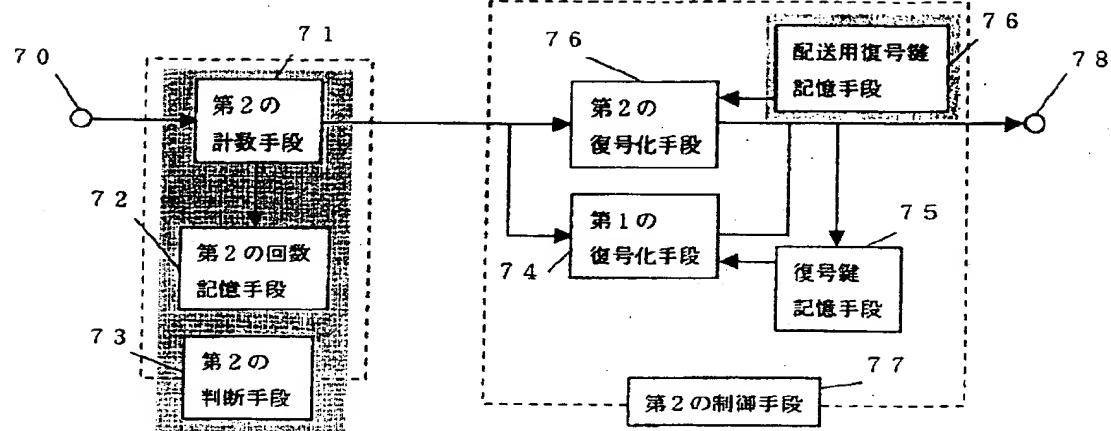


【図11】



【図12】

受信局



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.